INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/13109

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MENEZES A J ET AL: "HASH FUNCTIONS AND DATA INTEGRITY" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 321-383, XP002275660 ISBN: 0-8493-8523-7 page 321	1-31
X	US 4 309 569 A (MERKLE RALPH C) 5 January 1982 (1982-01-05) the whole document	1-31
X	US 4 881 264 A (MERKLE RALPH C) 14 November 1989 (1989-11-14) abstract page 10, line 41 - page 14, line 27	1-31

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 August 2004	31.08.04

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertolissi, E

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/13109

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 903 651 A (KOCHER PAUL CARL) 11 May 1999 (1999-05-11) abstract column 5, line 54 - column 8, line 13 figures 5-9	1-31
X	J. CHAPWESKE, G. MOHR: "Tree Hash EXchange format (THEX)" ONLINE DOCUMENT, 'Online! 4 March 2003 (2003-03-04), XP002283758 Retrieved from the Internet: URL:http://www.open-content.net/specs/draft-jchapweske-thex-02.html> 'retrieved on 2004-06-08! the whole document	1-31
X	R. BRANDNER, TOBIAS GONDROM, U. PORDESCH, M. TIELEMANN: "<draft-brandner-etal-ats-00.txt> - Archive Time-Stamps Syntax (ATS)" INTERNET-DRAFT, 'Online! June 2003 (2003-06), XP015000365 Retrieved from the Internet: URL:http://ftp.scarlet.be/pub/documentation/internet-drafts/draft-brandner-etal-ats-00.txt> 'retrieved on 2004-06-08! Abstract 3 Enhanced Time-Stamp 3.1-3.3	1-31
A	EP 0 932 109 A (YEDA RES & DEV) 28 July 1999 (1999-07-28) abstract	1-31
A	US 6 065 008 A (HITCHCOCK GREGORY ET AL) 16 May 2000 (2000-05-16) abstract	1-31
A	EP 1 164 746 A (MICALI SILVIO) 19 December 2001 (2001-12-19) abstract	1-31
X	PHIL ZIMMERMAN ET ALT: "Introduction to Cryptography (PGP 6.5 User's Guide)"'Online! 6 June 1999 (1999-06-06), XP002292241 Retrieved from the Internet: URL:ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf> 'retrieved on 2004-08-11! page 18 - page 33 page 45 - page 49	32-44, 61,62

-/--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/13109

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PATRICK FEISTHAMMEL: "Explanation of the web of trust of PGP"'Online! 19 June 2002 (2002-06-19), XP002292242 Retrieved from the Internet: URL:http://www.rubin.ch/pgp/weboftrust.en.html> 'retrieved on 2004-08-12! the whole document	32-44, 61,62
X	CARONNI G: "Walking the Web of trust" ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES, 2000. (WET ICE 2000). PROEEDINGS. IEEE 9TH INTERNATIONAL WORKSHOPS ON GAITHERSBURG, MD, USA 14-16 JUNE 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 14 June 2000 (2000-06-14), pages 153-158, XP010522927 ISBN: 0-7695-0798-0 Abstract 4 The web of trust	32-44, 61,62
A	KARL ABERER, ANWITAMAN DATTA, MANFRED HAUSWIRTH: "A decentralized public key infrastructure for customer-to-customer e-commerce" ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE TECHNICAL REPORT, 'Online! no. ic/2003/74, 20 November 2003 (2003-11-20), XP002292243 Retrieved from the Internet: URL:http://icwww.epfl.ch/publications/documents/IC_TECH_REPORT_200374.pdf> 'retrieved on 2004-08-11! Abstract 2 PKI approaches	32-44, 61,62
X	VAL HENSON: "An Analysis of Compare-by-hash" PROCEEDINGS OF THE HOTOS-IX FULL PROGRAM, 'Online! 12 May 2003 (2003-05-12), XP002292468 LIHUE, HAWAII Retrieved from the Internet: URL:http://www.nmt.edu/{val/review/hash.pdf> 'retrieved on 2004-08-13! abstract	45-60

-/--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/13109

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SRDJAN CAPKUN, LEVENTE BUTTYAN AND JEAN-PIERRE HUBAUX: "Self-Organized Public-Key Management for Mobile Ad Hoc Networks" ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE TECHNICAL REPORT, 'Online! no. ic/2002/34, 28 May 2002 (2002-05-28), XP002292469 Retrieved from the Internet: URL:http://icwww.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf> 'retrieved on 2004-08-13! Abstract 1 Introduction 3.2 Certificate exchange 3.3 Constructing updated certifacate repositories 3.4 Certificate revocation	45-60
A	FARID F. ELWAILLY AND ZULFIKAR RAMZAN: "QuasiModo: More Efficient Hash Tree-Based Certificate Revocation"'Online! 5 September 2003 (2003-09-05), XP002292470 Retrieved from the Internet: URL:http://www.docomolabs-usa.com/researchers/ZRamzan/quasi-modo-v1.pdf> 'retrieved on 2004-08-12! Abstract 1 Introduction	45-60
A	PREM DEVANBU, MICHAEL GERTZ, APRIL KWONG, CHIP MARTEL, GLEN NUCKOLLS, STUART G. STUBBLEBINE: "Flexible authentication of XML documents" PROCEEDINGS OF THE 8TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 'Online! 5 November 2001 (2001-11-05), pages 136-145, XP002292471 PHILADELPHIA, PA, USA Retrieved from the Internet: URL:http://www.stubblebine.com/01ccs-stubblebine.pdf> 'retrieved on 2004-08-16! Abstract	45-60

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP 03/13109

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-31

   Method and computer readable medium for managing digital data

   ---

2. claims: 32-44, 61, 62

   Method and computer readable mediumfor providing trust levels of signatures

   ---

3. claims: 45-60

   Method for provoding integrity and consistency information of digital data

   ---

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/13109

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 4309569	A	05-01-1982	NONE		
US 4881264	A	14-11-1989	NONE		
US 5903651	A	11-05-1999	AU	3124997 A	05-12-1997
			GB	2330504 A	21-04-1999
			WO	9743842 A1	20-11-1997
			US	6532540 B1	11-03-2003
			US	2002188843 A1	12-12-2002
			US	6442689 B1	27-08-2002
EP 0932109	A	28-07-1999	US	6226743 B1	01-05-2001
			EP	0932109 A2	28-07-1999
			IL	128040 A	04-01-2004
			JP	11289329 A	19-10-1999
US 6065008	A	16-05-2000	NONE		
EP 1164746	A	19-12-2001	US	6097811 A	01-08-2000
			EP	1164746 A2	19-12-2001
			AT	216820 T	15-05-2002
			AU	7526996 A	22-05-1997
			DE	69620904 D1	29-05-2002
			EP	0858702 A1	19-08-1998
			WO	9716905 A1	09-05-1997
			US	2002165824 A1	07-11-2002
			US	2003221101 A1	27-11-2003
			US	2004049675 A1	11-03-2004
			US	5717758 A	10-02-1998
			US	2002046337 A1	18-04-2002
			US	6301659 B1	09-10-2001
			US	6487658 B1	26-11-2002